International aspects of Common Criteria

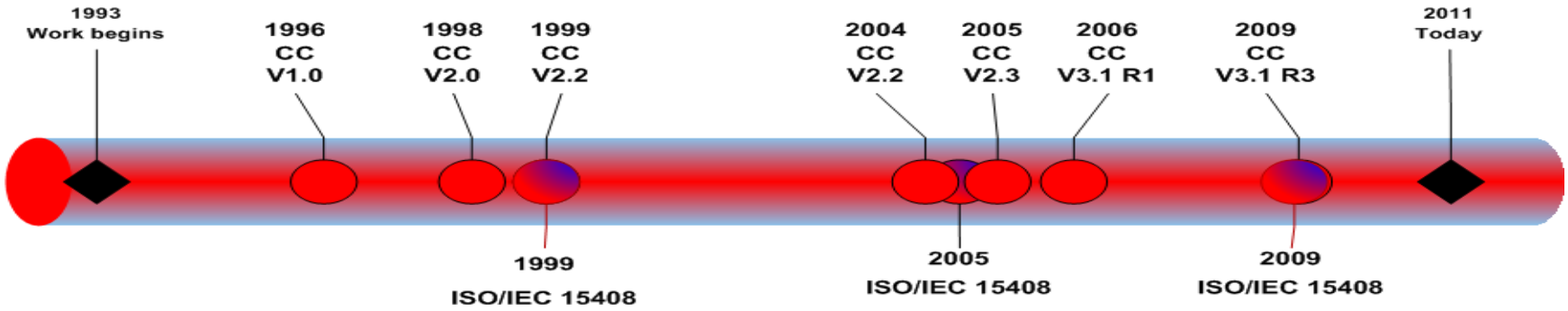
Fiona Pattinson.

Software Assurance Working Group

29th November, 2011

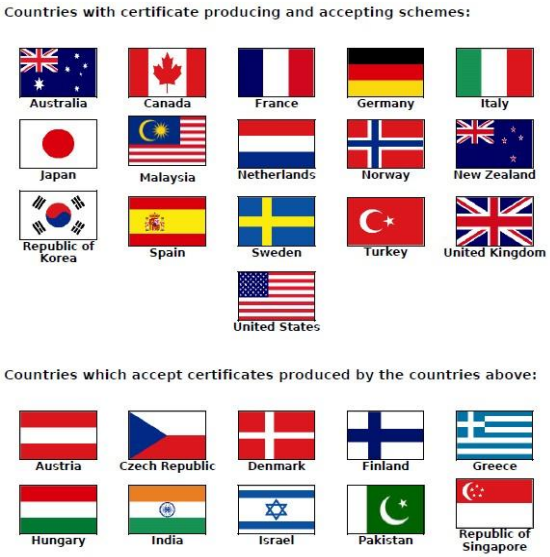
A short History of the CC

- Work on CC started in 1993
  - Harmonization of European ITSEC, US Federal Criteria, and Canadian CTCPEC
  - Was originally supposed to be done in ISO/IEC SC27 WG3
  - To speed up development, a separate group was founded:
    - the “Common Criteria Development Board” (CCDB)
  - Development took much longer than anticipated
    - First Version ready in 1996
  - It became an ISO Standard : ISO/IEC 15408 in 1999

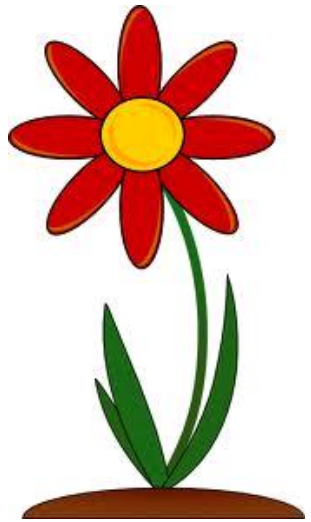


Mutual Recognition

- For the first time Security Certifications were internationally accepted!
  - Previously only ITSEC certifications were accepted all over Europe (SOGIS-MRA)
    - SOGIS = Senior Officials Group on Information Secur
  - First CC MRA signed on October 5, 1998 by:
    - France, Germany, United Kingdom, Canada, US
  - Today the CCRA is signed by 26 Nations
    - 16 Certification Schemes can issue certificates
  - Most large nations developing IT products have signed the CCRA, missing only China and Russia



Are the CC successful?



- Some CC Facts
  - Total number of certificates: 1600+
    - 823 in the last 4 years
    - 692 of those are at EAL4 or EAL4+
    - Over 400 vendors have successfully completed evaluations
    - Included most commercial operating systems and DBMS
    - Included most firewall systems, routers, access managers
    - Included practically all smart card chips and smart card operating systems
  - Accepted by 26 Nations (used by even more)
  - Regarded as “THE” standard for information assurance

What else does it take to be named successful?

Data from the CC portal 11/27/11 : http://www.commoncriteriaportal.org/products/stats/

Are the CC too successful?

- To some extent: yes
  - Many new schemes entered the CCRA
    - With little to no experience
  - Many products have been evaluated that shouldn't have been
    - No assurance, but they got "the stamp"
  - Evaluations focused on the wrong aspects
    - Checked for the existence of documentation rather than security
    - CEM supports this way of working
  - Not enough experienced evaluators and validators

Meanwhile, in ISO….

- Formal liaison with the CCDB
- Involvement from non-CCRA nations
- ISO/IEC 15408 and 18045: Updates and corrigenda
- Production of internationally demanded supporting documents
  - ISO/IEC TR 15446:2009: Guide for the production of Protection Profiles and Security Targets
  - ISO/IEC TR 19791:2010: Security assessment of operational systems
  - ISO/IEC 19792:2009: Security evaluation of biometrics
  - ISO/IEC PDTR 20004: Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
  - ISO/IEC WD TR 30104: Physical Security Attacks, Mitigation Techniques and Security Requirements
  - ISO/IEC 29128 :2011 Verification of cryptographic protocols
  - NWIP: Detailing software penetration testing under ISO/IEC 15408 and 18045 vulnerability analysis

A full list of the work program for SC 27 can be found at: http://tinyurl.com/SC27-list

CC Doesn't do supply chain?

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

IBM Corporation

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: IBM Global Security Kit V7.0.4.11
Evaluation Platform: AIX 4.3.3, 5.1, 5.2, 5.3; Solaris 7, 8, 9, 10; HPUX 11, 11i, 11iV2, 11iV3; Windows NT, XP, 2000, 2003, Vista; RHEL 2.1, 3, 4, 5; SLES 8, 9, 10 (for specific versions and patch levels see Section 2.4.3 in Security Target)

CCTL: atsec information security corporation
Validation Report Number: CCEVS-VR-07-0039
Date Issued: 2 August 2007
Assurance Level: EAL 4
Protection Profile Identifier: None

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Information Assurance Director
National Security Agency

- A CC V3.1 evaluation includes at least..
  - Precise specification of what is evaluated
    - The configuration, environment, assumptions and threat model
  - Evaluation of administrator and user guidance to assure that instructions and guidance match the product configuration
  - The delivery process (EAL 2 and above)
  - Delivery chain security (EAL3 and above)
  - Patching process (optional, but usually done)
  - Security of the development environment, well-defined configuration management
- The smart card industry supplemented CC for supply chain issues between smart card developer and customizing silicon suppliers.
- International vendors attempting further CC supply chain efforts in collaboration with CCDB

What do global vendors say?

- An internationally recognized evaluation scheme is vital
  - Nations (and commercial entities) will not give up asking for a proof of assurance
  - More nations in the line to sign the CCRA
  - Evaluate once, accept in many nations
    - Potentially a vendor needs to perform many evaluations using different criteria, schemes, labs.
    - This effects cost, time to market, reduces potential for supply chain issues (E.g. Is a product version honed for CC evaluation giving the same assurance as a similar version with a Russian certification?)
    - Potentially a vendor needs to disclose IP protected material to many entities in different countries (including China and Russia)
  - Don't use CC as a trade barrier
- Lack of progress in the CCDB will strengthen disparate IA programs
  - Mainly China,Russia and the UK – and they have a strategy!

The NIAP Palava

- National Information Assurance Partnership
  - Scheme, validator and lab support resources are critically limited
  - Two years since a US Govt PP only policy announced with (to date) only 5 PPs published
  - Little resource to produce good Standard U.S. PPs supporting U.S. policy – Recent US PPs are currently not even validated under the CC process.
  - NIAP's history of often changing strategy and sometimes ineffective policy changes have resulted in high risk to vendors thinking of investing in CC evaluation in the U.S.
  - Loss of evaluation and validation knowledge/skills within the U.S.

Global vendors

- So…many vendors went to other national schemes
  - Many vendors for components integrated into NSS and critical infrastructure are based in the U.S.
  - Critical infrastructure and non NSS users are not easily accepted by NIAP even though CC evaluation is highly recommended in those sectors. (CCRA can be used though)
  - Need to evaluate with the right assurance for an international market
  - EAL2, or mandatory use of poor PPs (not even validated) embodying national policy is not appropriate for key components internationally
    - E.g. core: OS, Virtualization-related, databases, network infrastructure
  - More experienced labs, abroad offer better service,
    - U.S. lab performance often cited as generally poor

See NIAP Policy #12: Letter of Intent (LOI) Requirement for Acceptance into CCEVS Evaluation

Summary

- More CCRA signatories especially from Asia in process
- ISO producing much supportive work used internationally
- CCDB promoting a collaborative PP (CPP) strategy
  - PPs are developed by Technical Communities
  - Different from the NIAP effort
- An initiative by global vendors to engage the CCDB in supply chain work
- At least China, Russia and the UK are developing IA schemes outside the CCRA
- NIAP history of policy change, current strategy and proposed policies are weakening the US position within the CCRA